



Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
User Group	Wed, Mar 16 9:00 to 12:00	GSA Central Office 1800 F St. NW Room 6044	888-455-1864 Passcode: 5887966
CAB	Wed, Apr 6 9:30 to 12:00	GSA Central Office 1800 F St NW Room 3042	No Telecon Provided
Registrar Refresher Training	Thu, Apr 14 2:30 to 3:30	Telecon/Webinar	888-455-1864 Passcode: 3611044
Registrar Classroom Training	Wed and Thu Apr 13-14 May 18-19 Jun 15-16	HPE Chantilly, VA	Contact Jim Schoening for information or to Register

Special Points of Note:

Now found on
www.fedidcard.gov:

- > Service Order Requests and Test Card Orders
- > Role Holder Web Based Training Registration
- > Deployment Activities and USAccess Center Status Alerts
- > Contact Ken Bandy (kenneth.bandy@gsa.gov) to be added to USAccess distribution lists.
- > Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up

USAccess Software Release 9.9 Pushed to Production

Release 9.9 was pushed to production as scheduled last Saturday, March 5. This release included the foreign national credentialing capability, editing SSN in Sponsorship, as well as rolling PCA out to the fixed workstations.

USAccess Light Installers v4.0, which was posted to the SFTP server on February 9, updates Light systems with these changes as well as installs PCA on LA and LCA machines.

The MSO has held several trainings for Sponsors, Registrars and Activations over the past two weeks, reaching over 1,800 role holders.

Inside this issue:

Meetings and Training Calendar	1
Spotlight Articles	1-3
Service Enhancements	3
Security Tip	4

USAccess Software Release 9.9 Continued

Updated job aids (Sponsor Quick Reference, Adjudicator Job Aid), as well as a PCA user guide are available on the Agency Lead Portal. The presentations used during Sponsor and PCA trainings are also posted.

The recordings of the Sponsor and PCA trainings will be posted to the ALP by early next week. A compilation of FAQs from the sessions will also be posted to the ALP.

Lastly, the USAccess Authoritative User Data Interface Guide is also on the ALP and assists SIP customers with credentialing foreign nationals and editing the SSN field.

Release 9.9 Known Issues Log

A USAccess Software Release 9.9 Known Issues document will be posted on the ALP and be available on Monday, March 14. This document lists the known issues, user impacts, and available workarounds until a fix is available. This document will be updated periodically.

Light Installer v.4.0.1 Details

We are prepping a Light Installer v4.0.1 to address known issues with v4.0. Please see the USAccess Software Release 9.9 Known Issues document posted on the ALP for more information on these issues.

An email will be sent next week announcing when the Light Installers v4.0.1 will be posted to the SFTP server. Testing is still occurring with this installer, and we don't want to release to the field until this is fully completed and any issues documented.

Once available, Agencies should apply this 4.0.1 installer to Light machines when available (even if v4.0 has been applied) to fix known issues with PCA in the field.

A draft Light Installers v4.0.1 release notice will be posted to the ALP by the end of this week.

Explore the Government Acquisition Gateway Yet?

The Acquisition Gateway, otherwise known as the Common Acquisition Platform (CAP) and built by GSA, helps federal government buyers from all agencies act as one acquisition community. The Acquisition Gateway features information on government-wide contract vehicle comparisons, acquisition best practices, market research tools, prices paid data, and other useful tools and features. Federal employees with a PIV card or approved contractors can access the site. Sign up at <https://hallways.cap.gsa.gov>

Service Enhancements

Changes/Updates since last Blue Top

- Routine maintenance was completed as scheduled on February 27-28.
- USAccess Software Release 9.9 was pushed to production as scheduled on March 5.
- Modified Zone 17 for NARA

Planned changes

For any maintenance downtime periods, please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.

- **Light installers v4.0.1**— will be made available on the SFTP server in the next few weeks and should be implemented on LA and LCS machines to take advantage of Release 9.9 and PCA features. Fixed workstations will be updated with this fix using the automated update system (no Agency action required other than to keep workstations powered on.)
- **Sunday, March 13 from 1am-4am Eastern**— There is routine maintenance scheduled and the USAccess service and portals will be unavailable during this time.
- **Saturday, March 26**—There is routine maintenance schedule for this day. The USAccess service and portals will be unavailable for most of the day.

Security Tip

Protecting Your Government Owned Equipment and Personally Identifiable Information

The USAccess PIN is a six (6) to eight (8) digit number known only by the cardholder and used to authenticate the cardholder to an agency enterprise IT network. Your USAccess PIV - something you have - and PIN - something you know - are key elements of the multi-factor security used to access government data and Public Key Infrastructure (PKI) certificates on your card's integrated computer chip. Your agency's logical or physical access systems may require the PIN to unlock the PIV card before you can successfully authenticate to the IT system. The PIV card and PIN is also employed if you are required to provide a digital signature.

PIN Best Practices

When creating your PIN it is recommended that you:

- Select a PIN that cannot be easily guessed (i.e., do not use birth date, partial account numbers, sequential numbers like 1234, or repeated values such as 1111).
- Null values (blanks) are not supported by USAccess, nor allowed by federal guidance
- Memorize your PIN. Do not write on your PIV card, a post-it note or on a piece of paper attached to your monitor or in your wallet.
- Do not use your PIN as a password for other non-government IT services such as your personal email or bank account.

Safeguarding Your PIN

The PIN should be kept secure at all times even though it is useless to others unless they also have physical control of your card. Because of the risk to your agency, and you, it is critical that you never share your PIN with trusted co-workers, subordinates, or superiors. Doing so will expose you to fraud and identity impersonation. USAccess recommends the following:

- Be aware of others that may be nearby when using your PIN. Observing the PIN you enter is the first step in compromising your identity.
- If you believe that your credential has been tampered with, lost or stolen report it immediately to your agency's Security Officer.